

REMARKS

Claims 1-11, 15-73 and 80-85 are pending. The Applicant respectfully requests consideration of the following remarks.

35 U.S.C. § 102(e) Rejections

Claims 80-84 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,200,864 to Hollingsworth (hereinafter “Hollingsworth”). The Applicant respectfully traverses the rejection.

Claim 80 recites a computer-implemented method comprising:

- retrieving a list of user accounts from an identity integration system having persisted identity information regarding the user accounts wherein, the identity integration system includes a management agent for each of multiple data sources configured specifically for its respective data source to manage data communication between the identity integration system and each respective data source;
- outputting a user interface showing the list of user accounts on a display;
- allowing each account in the list to be selected using a user interface selection device operable to input selections via the user interface output on the display;
- allowing input of a new password via the user interface selection device; and
- allowing input of a request to update old passwords associated with each of the selected accounts to the new password input via the user interface.

The Examiner asserts in rejecting claim 80 that Hollingsworth discloses “A computer-implemented method comprising: retrieving a list of user accounts (310) from an identity integration system...” *See Office Action, Page 4.* The cited portions of Hollingsworth are: “In the example shown in Fig. 3 system 300

includes an exemplary computer display that includes a list 310 of programs that are accessible by the universal system.”*See Hollingsworth, Col. 4, Lines 26-28.*

Hollingsworth does not in fact disclose either a list of user accounts or an identity integration system. Hollingsworth merely discloses a list of “programs that are accessible by the universal system” which are not the claimed feature of “user accounts”.

In addition, Hollingsworth’s “universal system” merely “...enables a user to control passwords of one or more programs that are in communication with the universal program”, *See Hollingsworth, Col. 2, Lines 54-56*, which is not the feature of an identity integration system “...having persisted identity information regarding the user accounts” and “a management agent for each of multiple data sources configured specifically for its respective data source”, as recited in claim 80. Hollingsworth’s more rudimentary system only has one function, and that is to very generally control passwords of one or more programs which is not the claimed feature of an entire multi-functional identity integration system with specifically configured management agents.

Claim 80 recites in part:

- the identity integration system includes a management agent for each of multiple data sources configured specifically for its respective data source to manage data communication between the identity integration system and each respective data source;

The Examiner asserts that Hollingsworth teaches a system which “includes a management agent” *See Office Action, Page 4*, and cites the following portion of

Hollingsworth, “Such secondary programs may need to have to be adjusted or edited to allow the universal program to access and change or otherwise edit the passwords of such secondary programs”, *See Hollingsworth, Col. 8, Lines 10-13.* The tiered system disclosed in Hollingsworth describes numerous adjustments and editing and in addition multiple tiers of multiple programs which is not the claimed feature of an “identity integration system include[ing] a management agent for each of multiple data sources configured specifically for its respective data source to manage data communication between the identity integration system and each respective data source”, *See Claim 80.*

Hollingsworth’s secondary programs which require editing and adjusting in order to merely allow the universal program to have access are not the claimed feature of a management agent “for each of multiple data sources” which is “configured specifically for its respective data source” and does not need to be specifically adjusted or altered as it is already specifically configured. Therefore, Hollingsworth’s universal program is merely a secondary program itself which may have to be altered and edited each time it communicates with a different program; in fact it functions more generally as opposed to having a specifically configured management function.

Claim 81 depends either directly or indirectly from claim 80 and is allowable as depending from an allowable base claim. Each of the dependent claims is allowable based on the same rationale discussed with respect to claim 80. These claims are also allowable for their own recited features which, in

combination with those recited in claim 80, are neither shown nor suggested in the references of record, either singly or in combination with one another. Withdrawal of the rejection is respectfully requested.

Claim 82 recites:

One or more computer readable storage media containing instructions that are executable by a computer to perform actions, comprising:

- selecting multiple data sources connected to an identity integration system;
- receiving a new password input by a user to cause the new password to be associated with each of the selected multiple data sources; and
- using the identity integration system to collectively update a password associated with each of the selected multiple data sources to the new password input by the user.

In rejecting claim 82, the Examiner asserts that Hollingsworth discloses, “...using the identity integration system col. 2 line 54-56; e.g universal access program for controlling passwords) to collectively update (col. 2 line 54-57 and col. 3 line 52) a password associated with each of the selected multiple data sources...” *See Office Action, Page 6.* The portions cited by the examiner are as follow, “The universal program enables a user to control passwords of one or more programs that are in communication with the universal program” *See Hollingsworth, Col. 2, Lines 54-56* and “...there is a need for a new system that streamlines the password control process such that the user will not have to spend inordinate amounts of time for setting, updating, or controlling passwords for various programs in communication with a central control program” *See*

Hollingsworth, Col. 3, Lines 48-53. In addition to a “universal program” not being an identity integration system (as discussed above), Hollingsworth also fails to disclose a system to “collectively update a password”. Hollingsworth merely describes a user controlling the passwords for one or more programs which is not even remotely the same as the collective updating of passwords.

Claims 83-85 depend either directly or indirectly from claim 82 and are allowable as depending from an allowable base claim. Each of the dependent claims is allowable based on the same rationale discussed with respect to claim 82. These claims are also allowable for their own recited features which, in combination with those recited in claim 82, are neither shown nor suggested in the references of record, either singly or in combination with one another.

For example, **Claim 84** recites, “The one or more computer readable storage media as recited in claim 82, wherein the identity integration system accomplishes a password update on each of the data sources regardless of whether the data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system”.

In rejecting claim 84, the Examiner asserts that Hollingsworth discloses, “...the one or more computer readable storage media as recited in claim 82, wherein the identity integration system accomplishes a password update on each of the data sources regardless of whether the data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system” *See Office Action, Page 6*, and

cites the following portion of Hollingsworth, “An exemplary system and method of the present invention includes a universal program that is in communication with one or more password-accessed programs, routines, or sub-routines. The universal program enables a user to control passwords of one or more programs that are in communication with the universal program” *See Hollingsworth, Col. 2, Lines 51-56.* Hollingsworth merely discloses enabling a user to control the passwords of one or more programs that are in communication with a universal program, and is silent as to the claimed feature of an identity integration system which updates passwords, “regardless of whether the data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system” *Claim 84.* In fact, Hollingsworth’s password control is potentially rendered useless in a system which has a different communication mode than the native communication mode.

As previously mentioned, Hollingsworth discusses a situation in which, “...secondary programs may have to be adjusted or edited to allow the universal program to access and change or otherwise edit the passwords of such secondary programs” *See Hollingsworth, Col. 8, Lines 10-13.* Therefore, unless such secondary programs can be edited or adjusted in such a way as to allow interaction between Hollingsworth’s universal program and secondary programs, no password control can be facilitated thus making Hollingsworth’s system entirely ineffectual. Withdrawal of the rejection is respectfully requested.

35 U.S.C. § 103(a) Rejections

Claims 1-11, 15-20, 22-69, 71-73 and 85 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hollingsworth as applied to claims 80-84 in view of U.S. Application No. 2003/0233439 to Stone et al (hereinafter “Stone”). The Applicant respectfully traverses the rejection.

Claim 1 recites:

1. A method, comprising:

outputting a user interface configured to interact with an identity integration system to perform collective password management for multiple user accounts associated with a user;

receiving a selection of selecting multiple data sources connected to an the identity integration system input by the user via the user interface, wherein:

each of the multiple data sources corresponds to a different one of said multiple user accounts;

the identity integration system includes a management agent for each of the multiple data sources configured specifically for its respective data source to manage data communication between the identity integration system and each respective data source;

for at least some of the multiple data sources a management agent for the data source is configured with credentials to perform password management for a corresponding said user account; and

for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source;

receiving a new password input by a user via the user interface; and

performing an administrative password operation on a multiple passwords each associated with each one of the selected multiple data sources to collectively update each said of the multiple passwords to the new password, wherein the password operation is performed using the identity integration system.

In rejecting claim 1, the Examiner asserts that Hollingsworth teaches, “...a management agent for each of the multiple data sources configured specifically for its respective data source” *See Office Action, Page 8* citing the following portion of Hollingsworth, “Also, the password would have the ability to change the password of all such secondary programs that are within communication with the universal program. Such secondary programs may need to have to be adjusted or edited to allow the universal program to access and change or otherwise edit the passwords of such secondary programs” *See Hollingsworth, Column 8, Lines 7-13.* Hollingsworth is in fact silent with regard to any type of a “management agent” or for that matter any kind of management system at all. Hollingsworth merely describes a password having the ability to change the password in secondary programs. Simple changing of passwords does not disclose a “management agent” that is “...configured specifically for its respective data source to manage data

communication between the identity integration system and each respective data source”.

Moreover, in the Examiner’s rejection of claim 1, the Examiner concedes correctly that “Hollingsworth does not expressly disclose for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source” *See Office Action, Page 8*. The Examiner asserts, however that Stone:

...teaches for at least one of the multiple data sources to be a management agent for the data source calls for custom logic configured as code (e.g. and [sic] XML file], from a custom logic source (administrator) outside the identity integration system, to perform password management for the data source. *See Office Action, Page 8*.

In making this assertion, the Examiner cites the following portion of Stone:

The central administration tool 14 allows an administrator to add new users to the directory services and new users to individual applications by means of a group membership. The group membership may be expressed as attribute data. If a user is moved to a directory services group, secondary security information or secondary application specific information is updated in a security component (e.g., 34) of the directory services system 32 and in a secondary security component (e.g., 38 or 52) associated with a resource. Where the applicable resource is an application, the secondary component data may be referred to generically as an application security store. *See Stone, ¶ 0038*

The Examiner asserts that an administrator is a custom logic source; Applicant respectfully disagrees. Stone’s administrator has one main function, “...to add new users to the directory services and new users to individual applications by means

of a group membership” *See Stone*, ¶ 0038. Merely adding users to directory services and applications is purely an administrative function and has nothing to do with custom logic. Therefore, an administrator acting in such a capacity lacks the ability to be a custom logic source. In addition, the Examiner uses the example of an XML file as custom logic, “...custom logic configured as code (e.g. and[sic] XML file)” *See Office Action, Page 8*. In fact, an XML file is not custom logic configured as code.

In Stone, the XML file merely serves as a data structure which is transmitted over the communications network to a directory interface and is processed to be compatible with a directory services system. For example, “The server 26 comprises a receiver 28, which is arranged to receive a transmission of a data structure 24 (e.g., an XML file), data packets, or another suitable data structure from the transmitter 20” *See Stone*, ¶ 0024.

A data structure such as an XML file lacks the ability to perform password management for the data source as it is merely a transmitted data structure which is processed. In fact, the data structure (XML file) in Stone is not operational at all as to function as it is only a transmitted file and as such, it is acted upon, not active. Therefore, Stone’s XML file is not capable of providing control over editing passwords for Hollingsworth’s multiple programs. The “user” in Stone is merely a user inputting data (not logic) in order to facilitate the server reading the contents of the data structure.

Claims 2-12 and 15-52 depend either directly or indirectly from claim 1 and are allowable as depending from an allowable base claim. Each of the dependent claims is allowable based on the same rationale discussed with respect to claim 1. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither shown nor suggested in the references of record, either singly or in combination with one another.

For example, with respect to **claim 11**:

The method as recited in claim 1, wherein for at least some of the multiple data sources the identity integration system stores integrated identity information to perform password management, the Examiner asserts that “Hollingsworth teaches the method as recited in claim 1 wherein for at least some of the multiple data sources the identity integration system stores integrated identity information to perform password management” *See Office Action, Page 11*. In rejecting claim 11, the Examiner cites the following portion of Hollingsworth, “Furthermore, the control program would decrease the need to memorize multiple passwords by electronically storing the passwords for the user” *See Hollingsworth, Col. 1, Lines 53-55*. Hollingsworth merely suggests a program which enables the user to store passwords and is silent as to storing integrated identity information to perform password management.

Claim 17 recites, “The method as recited in claim 16, wherein the selecting multiple data sources and the performing a password operation are performed on a website generated by the web application”.

In rejecting claim 17 and in addition, 16 and 18, the Examiner correctly asserts that “Hollingsworth does not expressly teach web application for password management” *See Office Action, Page 11*, and Examiner further cites Stone to correct this deficiency.

The Examiner states that “Stone teaches the method as recited in claim 16, wherein the selecting multiple data sources and the performing a password operation are performed on a website generated by the web application” *See Office Action, Page 12*. In rejecting claim 17, the Examiner relies on the following portion of Stone:

The directory services system 32 may be integrated or enhanced by the ancillary support module 39 such that the directory services system 32 support the provision of one or more of the following to clients 46: links to documents, web pages or other resources in an index, a table of contents or a topical hierarchy. In one embodiment, the topical hierarchy may be searchable or browsable. *See Stone, ¶ 0077.*

Stone merely describes user access to links to documents, web pages or other resources in an index, a table of contents or a topical hierarchy, and is absolutely silent with regard to any password operations being performed on a website generated by a web application and additionally, fails to even mention the use of passwords in conjunction with the described web links etc.

The Examiner rejected **claim 24**, “The method as recited in claim 22, wherein the interface allows a web application designer to customize the web application”, asserting that “Stone teaches he[sic] method as recited in claim 22,

wherein the interface allows a web application designer to customize the web application” *See Office Action, Page 14*. The Examiner relies on the following paragraph from Stone for this rejection:

The format converter-arranger 18 accepts the entered data from the entry data module 16 and converts or arranges the entered data into a file format or another data structure that is suitable for communication over the communication network 22. For example, format converter-arranger 18 may comprise an extensible markup language (XML) converter. The format converter-arranger 18 may be coupled to the transmitter 20. Extensible markup language is a specification for an electronic document or a file that is compatible for transmission over the internet or another communications network. XML defines the data structure that supports customization of tags to support the definition, transmission, validation, and interpretation of data between different entities or users. *See Stone ¶ 0021.*

Stone merely describes using an XML converter for the purpose of converting or arranging entered data into a suitable format for communication over a network. This conversion process has nothing to do with an interface which allows a web designer to customize a web application. Withdrawal of the rejection is respectfully requested.

The Examiner relies on both Hollingsworth as well as Stone in rejecting independent **claim 53**. Independent claim 53 recites:

An apparatus comprising:
a processor; and
a web application for password management executable on the processor
having one or more modules including:

a user identifier to find user identity information in an identity integration system, wherein:

the identity integration system includes a management agent for each of multiple data sources to manage data communication between the identity integration system and each respective data source; and

for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source;

identity information query logic to search information in the identity integration system for accounts associated with the user;

an account lister to display the accounts associated with the user;

an account selector to designate at least some of the displayed accounts for password management;

a password inputter to determine a new password input by a user to associate with each designated accounts; and

a password manager to collectively manage passwords for the designated accounts by requesting an update of a password associated with each designated account to the new password, responsive to the user input.

In rejecting claim 53, the Examiner again asserts that Hollingsworth teaches an “identity integration system” which includes “a management agent” *See Office*

Action, Page 19 and again cites the following portions of Hollingsworth, “The universal program enables a user to control passwords of one or more programs that are in communication with the universal program” *See Hollingsworth, Col. 2, 54-56* and “Such secondary programs may need to have to be adjusted or edited to allow the universal program to access and change or otherwise edit the passwords of such secondary programs *See Hollingsworth, Col. 8, Lines 10-13*. Applicant again, respectfully disagrees, for the same reasons as stated above with respect to Claim 1. The Examiner additionally rejects claim 53 on the basis that Stone teaches, “...a web application for password management (0040) for the entry attribute data for administering resources over a network” *See Office Action, Page 20.*

In making this rejection, the Examiner relies on the following portion of Stone:

In step S10, a user enters or selects attribute data or an attribute datum (e.g., an attribute value) associated with the user, a resource or both. Attribute data may define user attributes, resource attributes or both. A resource may refer to one or more of the following: the first resource 36, the second resource 50, another resource, an object, a printer, a router, a server, a database a network element, a computer program, and an application. The user may select or enter at least one attribute value or attribute from a user interface 12 coupled to the central administration tool 14. In one embodiment, the selection of an attribute data may occur by making entries on an electronic form or template that is displayable via the user interface 12. In such a case, the user interface 12 may comprise a browser (e.g. an Internet browser). In another embodiment, the user interface 12 supports a menu driven format for entry of attribute data. *See Stone, ¶ 0040.*

Stone merely describes the user inputting attribute data via an interface which may include a browser. Stone does not disclose the feature of using a web application for password management and in fact, fails to make any mention of password management at all. The Examiner also again relies on the XML file in Stone to reject claim 53 on the basis that Stone “...teaches for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code (e.g. and[sic] XML file), from a custom logic source (administrator) outside the identity integration system, to perform password management for the data source...” *See Office Action, Page 21.* Applicant again respectfully disagrees for the same reasons stated above with respect to claim 1. Withdrawal of the rejection is respectfully requested.

Claims 54-61 depend either directly or indirectly from claim 53 and are allowable as depending from an allowable base claim. Each of the dependent claims is allowable based on the same rationale discussed with respect to claim 53. These claims are also allowable for their own recited features which, in combination with those recited in claim 53, are neither shown nor suggested in the references of record, either singly or in combination with one another.

For example, in rejecting claim 54, which recites, “The apparatus as recited in claim 53, wherein the identity integration system connects with diverse data sources, each data source having a different function for using password security”, the Examiner relies on Hollingsworth, asserting that, “Hollingsworth teaches the apparatus as recited in claim 53, wherein the identity integration system connects

with diverse data sources, each data source having a different function for using password security” *See Office Action, Page 22*. The Examiner cites the following portion of Hollingsworth, “...includes exemplary secondary programs 121, 122, and 123. Each such program 121, 122, and 123 is further accessed through its own specific required password. Further, the program 111 in the first tier may have to be re-programmed with the passwords of each of the programs...” *See Hollingsworth, Col.3, Lines 1-5*. Hollingsworth is silent as to different functions existing for using password security. Hollingsworth merely discloses different programs which may have to be re-programmed, which use different passwords. In fact, Hollingsworth does not even necessarily suggest that these passwords are different, as in unique from another, only that each program must be accessed through its own password. Withdrawal of the rejection is respectfully requested.

Claim 61 recites:

An apparatus comprising a processor coupled to memory, the memory storing one or more modules executable via the processor to implement:

an interface for coupling an identity integration system with a password management web application;

logic for communicating with the identity integration system, wherein:

the identity integration system is capable of collectively updating a password on multiple data sources that use various functions of password updating responsive to input of a single new password by a user;

the identity integration system includes a management agent for each of the multiple data sources to manage data communication between the identity integration system and each respective data source;

for at least some of the multiple data sources a management agent for the data source is configured with credentials to perform password management; and

for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source;

logic for communicating with the password management web application;
logic for searching for objects in the identity integration system; and
logic for checking a connection status between the identity integration system and a data source,

The Examiner asserts that Hollingsworth teaches, "...the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords), wherein: the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) is capable of collectively updating a password (col. 4 line 37-40) *See Office Action, Page 23.* In rejecting claim 61, the Examiner relies on the following portion of Hollingsworth, "Optionally, an all system indicator box 316 may be provided that allows an operation to be performed on all systems in system column 310" *See*

Hollingsworth, Col. 4, Lines 37-40. Hollingsworth merely discusses the performance of a generic, unspecified operation on different systems and is silent with regard to collectively updating a password. Withdrawal of the rejection is respectfully requested.

Claims 62-64 depend either directly or indirectly from claim 61 and are allowable as depending from an allowable base claim. Each of the dependent claims is allowable based on the same rationale discussed with respect to claim 61. These claims are also allowable for their own recited features which, in combination with those recited in claim 61, are neither shown nor suggested in the references of record, either singly or in combination with one another. Withdrawal of the rejection is respectfully requested.

In rejecting **Claim 65**, examiner relies on substantially similar rationale as the Examiner used in the rejection of claim one, and Applicant respectfully disagrees for the same reasons stated above with respect to claim 1.

Claims 66-80 depend either directly or indirectly from claim 65 and are allowable as depending from an allowable base claim. Each of the dependent claims is allowable based on the same rationale discussed with respect to claim 65. These claims are also allowable for their own recited features which, in combination with those recited in claim 65, are neither shown nor suggested in the references of record, either singly or in combination with one another. Withdrawal of the rejection is respectfully requested.

Claims 21 and 70 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Hollinger (It is assumed that the Examiner meant Hollingsworth) and Stone as applied to claims 1-11, 15-20, 22-69, 71-73 and 85 above in view of U.S. Patent Application 2002/00883012 to Bush et al. (hereinafter “Bush”).

Claims 21 and 70 depend either directly or indirectly from claims 1 and 65 respectively and are allowable as depending from allowable base claims. Each of the dependent claims is allowable based on the same rationale discussed with respect to claims 1 and 65. These claims are also allowable for their own recited features which, in combination with those recited in claims 1 and 65, are neither shown nor suggested in the references of record, either singly or in combination with one another. The addition of the reference Bush, therefore, does not cure the deficiencies already discussed above with regard to claims 1 and 65. Withdrawal of the rejection is respectfully requested.

Conclusion

The Application is in a condition for allowance. The Applicant respectfully requests reconsideration and issuance of the present application. Should any issue remain that prevents immediate issuance of the application, the Examiner is requested to contact the undersigned attorney to discuss the unresolved issue.

Respectfully submitted,

Dated September 9, 2008

By: /William J. Breen, III/
William J. Breen, III
Reg. No. 45,313
509.755.7253

||